Eurocrypt 99

Pro mnohé byl 4. květen tohoto roku celkem obyčejným a nic neříkajícím dnem. Ne tak ale pro účastníky konference Eurocrypt 99, konané letos v Praze, mezi kterými by se napětí dalo doslova krájet.

RSA v ohrožení

Vše vyvrcholilo v 19.35 místního času, kdy v rámci večerního mítinku přednesl profesor Adi Shamir (pokud byste náhodou nevěděli, co znamená zkratka RSA, je to právě trojlístek Rivest – Shamir – Adleman) svůj referát na téma: “Faktorizace velkých čísel pomocí zařízení TWINKLE”. Jakmile referát skončil, všeobecné napětí se poněkud uvolnilo a první obavy z toho, že od zítra bude možné všechny kryptosystémy s RSA vyhodit, se rozplynuly, nicméně pocit, že něco divného visí ve vzduchu, ještě nějakou dobu přetrvával…

O co vlastně šlo? Jak víme, problém rozkladu velkých čísel na součin prvočísel (tzv. problém faktorizace) je hlavním pilířem, o nějž se opírá bezpečnost asymetrického kryptosystému RSA. Proto se také mezi kryptoanalytiky pořádají doslova závody, komu se podaří faktorizovat co nejdelší číslo. Dosavadní rekord je z letošního února a činí 465 bitů. Díky Shamirovu zařízení, které umožňuje proces faktorizace zrychlit zhruba tisíckrát, by se tato hranice mohla posunout o nějakých 100 až 200 bitů směrem nahoru. To by potom vážně ohrozilo systémy s klíčem o délce 512 bitů, což je v současnosti maximální velikost, která je povolena na export z USA. Profesor ve svém materiálu uvádí, že 95 % elektronického obchodu na internetu je chráněno právě klíčem délky 512 bitů. Pokud by se podařilo zařízení s názvem TWINKLE sestrojit (zatím jde o teoretický návrh, ale vypadá dost reálně), bylo by možné těchto 95 % komunikačních kanálů rovnou odepsat. Cena jednoho zařízení by přitom činila neuvěřitelných 5000 USD, přičemž pro rozklad 512 bitů je jich třeba 15 až 20 (pak by celá operace trvala devět až deset týdnů).

Abychom však zabránili šíření paniky, je třeba podotknout, že zmíněných 512 bitů je již delší dobu považováno za hazard (ostatně, proč by USA takový klíč jinak dovolily exportovat?). Profesionální systémy by měly používat klíč o velikosti alespoň 1024 bitů, přičemž pro vyšší stupeň bezpečnosti (certifikační autority apod.) je doporučováno rovnou 2048 bitů. Klíče o této velikosti zatím nejsou napadnutelné, a to ani při použití zmíněného zařízení.

Podívejme se nyní v krátkosti, jak TWINKLE (The Weizmann Institute Key Locating Engine) vlastně pracuje.

Nejprve pár slov o tzv. sieve-based algoritmech, které mohou TWINKLE urychlit. Základní myšlenka faktorizace nějakého čísla n zde vychází z následujícího pozorování: známe-li řešení kongruence $\mathbf{x}^2 \equiv y^2 \pmod n$, které je netriviální, tj. $x \neq \pm y \pmod n$, potom platí, že $\gcd(x - y, n)$ je faktorem čísla n. Pro nalezení zmíněné kongruence je třeba vygenerovat velké množství “pomocných” čísel, která je možné kompletně faktorizovat na určité množině prvočísel. K tomu se používají takzvané prosévací metody, jejichž efektivita přímo určuje složitost celého algoritmu.

Například pro faktorizaci 465bitového čísla trvaly operace prosévání na 200 počítačích kolem čtyř týdnů. A právě zde přichází ke slovu TWINKLE, představující masivní prosévací zařízení, pracující v násobku stovek až tisíců rychleji než běžně dostupný hardware. Jádrem zařízení je matice diod LED, z nichž každá odpovídá jednomu prvku z množiny určených prvočísel. Řídicí logika LED postupně vytváří různé kombinace obrazců a fotodetektor, oddělený logaritmickým filtrem, sleduje intenzitu výsledného záření. Přesáhne-li intenzita určitou hranici, je připojený počítač informován o nově "prositém" čísle (jeho kvalitu je ještě třeba ověřit, ale na to má počítač dost času). Pro řízení diod se předpokládá taktovací frekvence 10 GHz (při technologii GaAs) – odtud uvedený rychlostní nárůst.

Souhrnně je Shamirův projekt zajímavý zejména pro svou teoretickou hodnotu, přičemž akutní hrozbu pro kvalitně navržené kryptosystémy RSA nepředstavuje a ani v brzké době asi představovat nebude.

Tomáš Rosa,

tomas.rosa@decros.cz